PATENT ABSTRACTS OF JAPAN

(11)Publication number : **06-125554**
(43)Date of publication of application : **06.05.1994**

(51)Int.Cl. **H04N 7/167**
H04K 1/00
H04L 9/28
H04N 7/20

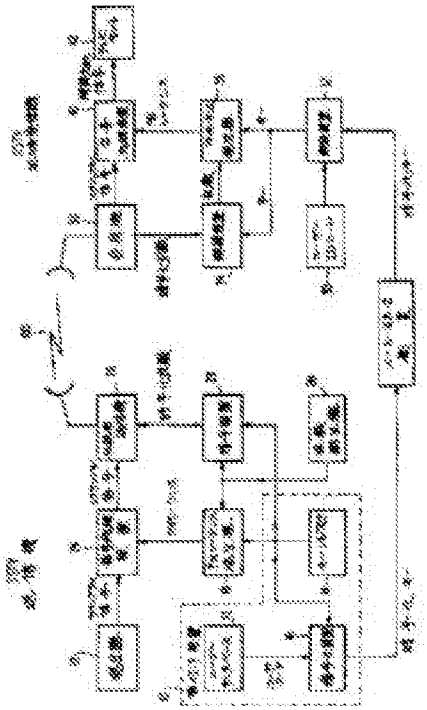
(21)Application number : **04-332267**
(22)Date of filing : **19.11.1992**

(71)Applicant : **COMMUNICATIONS SATELLITE CORP <COMSAT>**
(72)Inventor : **RIN NAN LEE**
RUSSELL J FUN

(30)Priority
Priority number : **81 322833** Priority date : **19.11.1981** Priority country : **US**

(54) PROTECTIVE METHOD OF CIPHERING FOR SUBSCRIPTION SATELLITE TELEVISION

(57)Abstract:
PURPOSE: To prevent nonsubscribed particles and subscribed parties delinquent in paying charges from receiving satellite television by using a ciphering technology by which video signals are transmitted to each subscribed party in different ciphered forms.
CONSTITUTION: A ciphered key ciphered by means of the ciphering device 16 of a programming device 10 is transmitted to a subscriber. The random number generator 20 of a transmitter periodically generates a new random number. A program signal from a supply source 22 is supplied to a signal processor 25 which ciphers the signal by using a divided PN sequence from an PN sequence generator. Ciphered signals are supplied to a transmission requiring transmitter 26 and a random number ciphered by means of a ciphering device 28 is also supplied to the transmitter 26 and transmitted together with the ciphered signals. The



decoder 32 of an image receiver 36 decodes the ciphered key. A receiver 36 separates the ciphered signals and supplies the signals to a decoder 34 which decodes the signals by using the key received from the decoder 32. The decoded signals are supplied to the television set 42 of the subscriber.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－125554

(43)公開日　平成６年(1994)５月６日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ　7/167		8943－5C		
Ｈ０４Ｋ　1/00		7117－5K		
Ｈ０４Ｌ　9/28				
Ｈ０４Ｎ　7/20		8943－5C		
		7117－5K	Ｈ０４Ｌ　9/ 02	Ａ

審査請求　有　　発明の数10(全　8　頁)

(21)出願番号　特願平4－332267
(62)分割の表示　特願昭58－500335の分割
(22)出願日　昭和57年(1982)11月19日

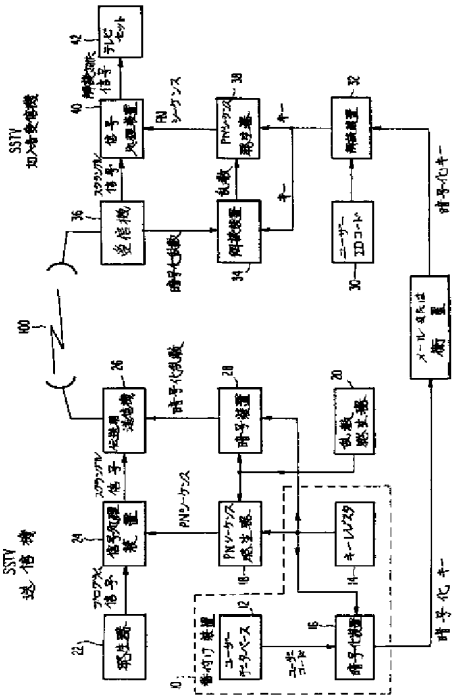
(31)優先権主張番号　３２２－８３３
(32)優先日　1981年11月19日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　593002436
コミュニケーションズ・サテライト・コーポレーション
COMMUNICATIONS SATELLITE CORPORATION
アメリカ合衆国　ワシントン、デイー・シー　20024、エス・ダヴリュ、レンフアント・プラザ　950
(72)発明者　リン・ナン・リー
アメリカ合衆国　メリーランド　20767、ジヤーマンタウン、イーグルス・ルースト・ドライヴ　18515
(74)代理人　弁理士　萩野　平　（外３名）

最終頁に続く

(54)【発明の名称】　加入衛星テレビジョン暗号化用防護方法

(57)【要約】　（修正有）
【目的】　加入衛星テレビジョンの料金滞納者および非加入者の受信を防護用のシステムを提供する。
【構成】　キーレジスタ１４からのキー数信号と乱数発生器２０からの第１シーケンス信号の乱数とを第２シーケンス発生器１８で暗号化した第２シーケンス信号と、発生器２２から出るプログラム信号をを信号処理装置２４において混合してスクランブル信号を作り、これと暗号装置２８においてキー数信号を前記乱数により暗号化した乱数とを伝送用送信機２６で混合した電波を衛星に向けて発射し、加入者は暗号化されたユーザＩＤ信号からキー数信号のみを解読装置１２により解読し、これにより衛星からの暗号乱数化されたスクランブル信号を受信機３６、解読装置３４、第２シーケンス信号発生器３８を介して第２シーケンス信号を得て受信機からのスクランブル信号を信号処理装置４０で解読してテレビセット４２に映像、音声を再現する。



1

【特許請求の範囲】
【請求項１】　送信機及び受信機間の信号伝送方式に於ける防護を付与する方法であって、
情報を示すプログラム信号を供給し、
第１シーケンスの数を示す第１シーケンスの信号を発生し、
キー数を示すキー数信号を供給し、
少なくも前記第１シーケンスの信号に従って前記プログラム信号を暗号化し、
暗号化された第１信号シーケンスを供給するために前記キー数信号により前記第１シーケンスの信号を暗号化し、
前記暗号化されたプログラム信号及び前記暗号化された第１信号シーケンスを前記受信機に送信し、
第３の信号に従って前記キー数信号を暗号化し且つ該第３の信号を前記受信機に伝達する段階とから成る送信方法と、
前記第１シーケンスの信号がキー数信号により暗号化されており、
第３の信号に応じて暗号化されたキー数信号を解読して供給し、
解読された第１信号シーケンスを得るために前記キー数に従って前記第１信号シーケンスを解読し、
前記プログラム信号を得るために少なくも前記第１信号シーケンスに従って前記暗号化されたプログラム信号を解読する段階とから成る受信方法とから成る方法において、
少なくも前記第１シーケンスの信号に従って前記プログラム信号を暗号化する段階が第２シーケンスの数を示す第２シーケンスの信号を発生する段階及び前記第２シーケンスの信号に従って前記プログラム信号を暗号化する段階とから成り、前記第２シーケンスの信号が少なくも前記第１信号シーケンスから成る送信リセット信号により各々始まる複数のシーケンスセグメントから成っており、
前記暗号化されたプログラム信号を解読する段階が少なくも解読された第１信号シーケンスから成る受信リセット信号で受信機シーケンス発生器を周期的にリセットすることにより前記第２シーケンスの数を示す解読シーケンス信号を発生する段階及び前記解読シーケンスに従って前記暗号化されたプログラム信号を解読する段階とから成る方法。
【請求項２】　前記送信及び受信リセット信号は各々前記キー数信号及び前記第１シーケンスの信号の組み合わせから成る請求項１に記載の方法。
【請求項３】　送信機により送信された暗号化信号を受信する複数の受信機を含み夫々の前記受信機は唯一の識別数を有し、前記第３の信号は個々の受信機に前記暗号化されたキー数を伝達するための前記唯一の識別数を示す識別数信号から成る請求項１に記載の方法。

2

【請求項４】　前記第３の信号は通常の操作による通信の間固定されている請求項１に記載の方法。
【請求項５】　前記キー数信号を発生する段階が前記キー数信号の周期的な変化から成る請求項１に記載の方法。
【請求項６】　前記キー数信号は前記第１シーケンスの信号よりも遅い割合で変化する請求項５に記載の方法。
【請求項７】　前記第２シーケンスの信号は非直線偽乱数シーケンスである請求項１に記載の方法。
【請求項８】　前記第１シーケンスは実質的に乱数シーケンスを示す請求項７に記載の方法。
【請求項９】　１つの信号通信方式に於いて送信機と受信機間で信号を伝達する方法であって、
情報を示すプログラム信号を供給し、
第１シーケンスの数を示す第１シーケンスの信号を発生し、
キー数を示すキー数信号を供給し、
第２シーケンスの数を示す第２シーケンスの信号を発生し、
前記第２シーケンスの信号が送信リセット信号で夫々始まる複数のシーケンスセグメントからなり、
前記送信リセット信号が前記キー数信号及び第１シーケンスの信号の組み合わせから成っており、前記第２シーケンスの信号に従って前記プログラム信号を暗号化し、
暗号化された第１信号シーケンスを供給するために前記キー数信号により前記第１シーケンスの信号を暗号化し、
前記暗号化されたプログラム信号と前記暗号化された第１信号シーケンスを送信する段階とから成る送信方法と、
前記第１シーケンスの信号がキー数信号によって暗号化されており、
前記キー数信号を供給し、
解読された第１信号シーケンスを得るために前記キー数に従って前記第１信号シーケンスを解読し、
第２シーケンスの数を示す第２シーケンスの信号を発生し、
前記第２シーケンスの信号は受信リセット信号により夫々始まる複数のシーケンスセグメントから成り、
前記受信リセット信号が前記キー数信号と前記解読された第１シーケンスの信号の組み合わせから成っており、
前記プログラム信号を得るために前記第２信号シーケンスに従って前記暗号化されたプログラム信号を解読する段階とから成る受信方法とから成る方法。
【請求項１０】　信号を送信する方法であって、
情報を示すプログラム信号を供給し、
第１シーケンスの数を示す第１シーケンスの信号を発生し、
キー数を示すキー数信号を供給し、
第２シーケンスの数を示す第２シーケンスの信号を発生

し、
前記第２シーケンスの信号は送信リセット信号で夫々始まる複数のシーケンスセグメントから成り、
前記送信リセット信号が前記キー数信号及び第１シーケンスの信号の組み合わせから成っており、　前記第２シーケンスの信号に従って前記プログラム信号を暗号化し、
暗号化された第１信号シーケンスを供給するために前記キー数信号により前記第１シーケンスの信号を暗号化し、
前記暗号化されたプログラム信号と前記暗号化された第１信号シーケンスを送信する段階とからなる送信方法。

【請求項１１】　少なくも第１シーケンスの数を示す第１シーンスの信号に従って暗号化されたプログラム信号を受信する方法であって、
前記第１シーケンスの信号がキー数信号によって暗号化されており、
前記キー数信号を供給し、
解読された第１信号シーケンスを得るために前記キー数に従って前記第１信号シーケンスを解読し、
第２シーケンスの数を示す第２シーケンスの信号を発生し、
前記第２シーケンスの信号が受信リセット信号により夫々始まる複数のシーケンスセグメントから成り、
前記受信リセット信号が前記キー数信号と前記解読された第１シーケンスの信号の組み合わせから成っており、
前記プログラム信号を得るために前記第２信号シーケンスに従って前記暗号化されたプログラム信号を解読する段階とから成る受信方法。

【請求項１２】　１つの信号通信方式に於いて送信機から受信機への信号を伝達する方法であって、
情報を示すプログラム信号を供給し、
前記情報を受信する全ての受信機に共通の第１シーケンスの数を示す第１シーケンスの信号を発生し、
前記情報を受信する全ての受信機に共通のキー数信号を供給し、
少なくとも前記第１シーケンスの信号に従って前記プログラム信号を暗号化し、
暗号化された第１信号シーケンスを供給するために前記キー数信号により前記第１シーケンスの信号を暗号化し、
前記暗号化されたプログラム信号と前記暗号化された第１信号シーケンスを送信する段階とからなる送信方法と、
前記キー数信号を供給し、
解読された第１信号シーケンスを得るために前記キー数に従って前記第１信号シーケンスを解読し、
前記プログラム信号を得るために前記第１信号シーケンスに従って前記暗号化されたプログラム信号を解読する段階とから成る受信方法とから成る方法。

【請求項１３】　信号送信方法であって、
情報を示すプログラム信号を供給し、
前記情報を受信する全ての受信機に共通の第１シーケンスの数を示す第１シーケンスの信号を発生し、
前記情報を受信する全ての受信機に共通のキー数信号を供給し、
少なくとも前記第１シーケンスの信号に従って前記プログラム信号を暗号化し、
暗号化された第１信号シーケンスを供給するために前記キー数信号により前記第１シーケンスの信号を暗号化し、
前記暗号化されたプログラム信号と前記暗号化された第１信号シーケンスを送信する段階とからなる方法。

【請求項１４】　少なくも前記プログラム信号を受信する全ての受信機に共通の第１シーケンスの数を示す第１シーケンスの信号に従って暗号化されたプログラム信号を受信し、且つ前記プログラム信号を受信する全ての受信機に共通のキー数を示すキー数信号により暗号化された前記第１シーケンスの信号を受信する方法であって、
前記キー数信号を供給し、
解読された第１信号シーケンスを得るために前記キー数に従って前記第１信号シーケンスを解読し、
更に前記プログラム信号を得るために前記第１信号シーケンスに従って前記暗号化されたプログラム信号を解読する段階とから成る受信方法。

【請求項１５】　１つの信号通信方式に於いて送信機から受信機へ信号を伝達する方法であって、
情報を示すプログラム信号を供給し、
少なくとも毎分数回変化する第１シーケンスの数を示す第１シーケンスの信号を発生し、
キー数を示すキー数信号を供給し、
少なくとも前記第１シーケンスの信号に従って前記プログラム信号を暗号化し、
暗号化された第１信号シーケンスを供給するために前記キー数信号により前記第１シーケンスの信号を暗号化し、
前記暗号化されたプログラム信号と前記暗号化された第１信号シーケンスを送信する段階とから成る送信方法と、
キー数信号を供給し、
解読された第１信号シーケンスを得るために前記キー数に従って前記第１信号シーケンスを解読し、
前記プログラム信号を得るために前記第１信号シーケンスに従って前記暗号化されたプログラム信号を解読する段階とから成る受信方法とから成る方法。

【請求項１６】　信号送信方法であって、
情報を示すプログラム信号を供給し、
少なくも毎分数回変化する第１シーケンスの数を示す第１シーケンスの信号を発生し、
キー数を示すキー数信号を供給し、

少なくとも前記第１シーケンスの信号に従って前記プログラム信号を暗号化し、
暗号化された第１信号シーケンスを供給するために前記キー数信号により前記第１シーケンスの信号を暗号化し、
更に前記暗号化されたプログラム信号と前記暗号化された第１信号シーケンスを送信する段階とから成る方法。
【請求項１７】　前記第１シーケンスの数がほぼ毎秒１回変化する請求項１６に記載の方法。
【請求項１８】　少なくも毎分数回変化する第１シーケンスの数を示す少なくとも第１シーケンスの信号に従って暗号化されたプログラム信号を受信する方法であって、
キー数信号を供給し、解読された第１信号シーケンスを得るために前記キー数に従って前記第１信号シーケンスを解読し、
前記プログラム信号を得るために前記第１信号シーケンスに従って前記暗号化されたプログラム信号を解読する段階とから成る受信方法。
【請求項１９】　前記第１シーケンスの数がほぼ毎秒１回変化する請求項１８に記載の方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、テレビジョン信号伝送の機密性に関し、詳言すれば、テレビジョン信号伝送の非公認受信の防御に関するものである。本発明を広く適用し得ることができかつそれに関連して本発明がここで説明される環境は加入者テレビジョンおよびテレビジョンプログラム分配についてのものである。
【０００２】加入者テレビジョン方式は益々普及してきており、このような方式においてテレビジョン信号はケーブル網を経由してまたは空中に送信されかつ月決め料金を支払った加入者のみによって受信されかつ聴視される。加入者テレビジョン方式が増大することによって、同様にプレミアムテレビジョンプログラムを料金を支払わずに受信しかつ映し出そうとする者の数も増大してきている。したがって、このような非公認の受信を防止するためのより複雑な防護技術に関する要求がある。
【０００３】現存する多くの加入者テレビジョン方式は、直接または間接的に衛星を経由して伝送される信号を利用し、そしてそれはテレビジョン受信専用（ＴＶＲＯ）アンテナを経由してプレミアムテレビ番組を受信して映し出すような不払いの個人に関して全く共通となっており、したがって加入テレビ番組の分配者の実質的な収入損失を結果として生ずる。加えて、種々の直接衛星放送テレビジョン方式が現在提案されておりこの方式において加入テレビ番組は個々の加入者の家庭へ衛星を経由して直接放送されるであろう。これらの加入衛星デレビジョン（ＳＳＴＶ）方式は非公認受信に対して確かに弱味があり、そしてそれゆえ有効な防護技術が非常に望まれる。

【０００４】ＳＳＴＶ方式用防護補助装置の目的は分配者の営業利益を保護することであり、かつしたがって以下の目的が達成されるべきである。
（１）非加入者が通常の家庭用テレビセットを使用することにより明白な映像および音声信号を受信するのを阻止すること。
（２）義務を怠る加入者がＳＳＴＶデコーダを使用して明白な映像および音声信号を受信するのを阻止すること。
【０００５】（３）正当な加入者が加入してないＳＳＴＶチャンネルまたはプログラムの明白な映像および音声信号を受信するのを阻止すること。
（４）平均的な技術者が受容し得る品質の映像および音声信号を得ることができる所有の受像機を作るのを阻止すること。
（５）小規模の非公認の営利会社がＳＳＴＶチャンネルから受容し得る品質の映像および音声信号を受信して映し出すことができる装置を製造して市販するのを阻止すること。
【０００６】（６）正当な加入者に高品質の映像および音声信号を加入チャンネルまたはプログラムから受信させかつ映し出させしめること。
また、上記目的を高くないコストで達成することが非常に望ましい。ＣＡＴＶについては多数の防護装置が存在し、その多くは伝送前に映像信号から水平同期パルスを抑制または除去し、かつ受信端で同期パルスを回復することを伴なう。これらの技術は同期回復回路を有してない人がプログラムを受信しかつ映し出すのを阻止し、そしてそれゆえ上記の目的（１）および（６）を達成するが、これらの防護装置は目的（２）および（３）を達成せず、そして同期回復回路は比較的容易に設計されかつ製造されるので、同様に目的（４）および（５）を満足させない。
【０００７】より複雑な技術は加入者のデコーダボックスに追加の情報を含むことができ、このデコーダボックスは個々の加入者に特別にアドレスされかつ幾つかのまたはすべてのチャンネルをオンまたはオフするのに使用される制御センタからの命令を受信する能力を含んでいる。これらのより複雑な防護技術は目的（１）～（３）および（６）を達成することには成功するかも知れないが、まだ目的（４）および（５）を満足させない。例えば、これらの技術の多くは合言葉のチェックを伴ない、そして特定のチャンネルが合言葉が整合された場合にのみオンされる。これは加入者のデコーダボックスを変更するかまたはオン／オフスイッチ以外のすべての必要な特徴をもつ別個のボックスを作ることにより比較的容易に回避されることができる。さらに、加入者は同様に実際に代価が支払われるより多くのプログラムを受信すべくデコーダボックスを不正に変更することができるかも

知れない。

【０００８】

【目的と発明の手段及び作用】本発明の目的は、上述した目的（１）～（６）のすべてが達成される加入テレビジョン方式用防護補助装置を提供することにある。本発明のさらに他の目的はコストおよび複雑さを最小にするかかる防護補助装置を提供することにある。

【０００９】これらおよび他の目的は映像信号の暗号化および解読に関して暗号技術を使用することによって本発明により達成される。暗号化（scrambling）および解読（descrambling）技術は規則的な根拠で変化されかつ支払済み加入者にのみ送られる「キー」を利用し、そして同様にこの「キー」は義務を怠る加入者が他から現行のキーを教わることができないように各加入者に対して異なる暗号化された形で送られる。

【００１０】記録は各加入者に対応する単独のユーザーＩＤ（識別）コードについて保持され、そして本発明の好適な実施例による送信機においては、キーは各加入者にキーを送る前にその加入者の唯一のＩＤコードで暗号化（ciphered）される。送信機中の乱数発生器は規則的な間隔で、例えば毎秒、新たな乱数を発生し、この数はキーと組み合され、そして次いで組み合された数が毎秒ＰＮシーケンス発生器をリセットするような発生源として使用される。

【００１１】したがって、このＰＮシーケンス発生器は１秒セグメントの任意発生源によりＰＮシーケンスを発生し、そして分けられたＰＮシーケンスは音声および映像プログラム信号を暗号化するのに使用される信号処理装置に供給される。乱数発生器はまたキーにより暗号化されかつ暗号化された乱数は暗号化された映像信号とともに連続的に送信される。

【００１２】受信機において、衛星（satellite ）またはメール（mail）を経由して送られた解読（deciphered）キーが特定加入者の唯一のＩＤコードを利用する受信機内で解読され、そのＩＤコードは受信機の内部にあり、かつ加入者には解らない。次いで暗号化されたキーは順次暗号化されたプログラム信号とともに受信された暗号化された乱数を解読するのに使用される。次に解読されたキーおよび乱数は送信機におけると同様に組み合され、そして組み合された信号は分けられたＰＮシーケンスが送信機に発生されたＰＮシーケンスに一致する受信機に発生されるように送信機のＰＮシーケンスと同一のＰＮシーケンス発生器を連続的にリセットするように使用され、そしてこの分けられたＰＮシーケンスは次いで受信信号を暗号化するように使用されることができる。暗号化された信号は次いで加入者のテレビジョンセットに供給される。

【００１３】

【実施例】図面は本発明によるＳＳＴＶ防護装置の機能的ブロック図を示す。ＳＳＴＶ送信機は代表的には支払済み加入者およびそれらに対応する唯一のユーザーＩＤコードのリストを含んでいる加入者情報を記憶する番付け（dilling ）装置用コンピュータ１０へのアクセスを含むかまたは有している。この情報は代表的にはコンピュータ内のユーザーデータベース１２内に記憶されても良い。またコンピュータ内にはレジスタ１４または規則的な根拠、例えば月毎に変化されるキーを含んでいる同等物がある。この「その月のキー」を各現行の加入者に送る用意に、キーはその特定の現行の加入者に唯一のユーザーＩＤコードにより暗号化装置１６で暗号化され、そして暗号化キーは次いで加入者に送られる。

【００１４】送信機は偽乱数（ＰＮ）シーケンス発生器１８および乱数発生器２０を含んでいる。該乱数発生器２０は新たな乱数を、例えば毎秒１つを周期的に発生し、そして乱数数発生器２０およびキーレジスタ１４の出力は組み合わされかつ従来技術において公知の方法でＰＮシーケンス発生器１８を周期的にリセットするかまたは「シード（seed）」するようにＰＮシーケンス発生器１８に付加される。シーケンス発生器１８の各シーディング（seeding)はＰＮシーケンスの新たな分割（セグメント）を始める。

【００１５】供給源２２からのプログラム信号は発生器１８からの分割されたＰＮシーケンスにより暗号化される信号処理装置２４に供給される。使用される暗号化（インクリプション）技術は種々の公知の技術のうちの１つであってもよくかつここで詳細に説明する必要はない。次いで、暗号化（インクリプトまたはスクランブル）された信号は種々の加入者受信機へのリンク１００を介して伝送用送信機２６に供給される。

【００１６】発生器２０からの乱数は暗号装置（encipherer）２８においてその月のキーにより暗号化されかつ暗号化された乱数はリンク１００を介して伝送用送信機２６に供給され。発生器２０からの乱数は暗号装置（encipherer）２８においてその月のキーにより暗号化されかつ暗号化された乱数はリンク１００を介して暗号化された映像信号とともに送信される。

【００１７】受信機において、レジスタ３０または加入者ＴＶ受像機の内部の同等物は据付け前にセットされかつ送信機においてビリングコンピュータのユーザーデータベース１２に記憶される加入者の特別な秘密のユーザーＩＤコードを含んでいる。したがって、加入者の受像機が暗号化（インサイファ）されたキーを受信するときまたはユーザーが暗号化されたキーをメールで受け取りかつ該暗号化キーを受像機に挿入するとき、受像機の解読装置（decipherer）３２はその特定の加入者に対して特別な秘密のユーザーＩＤコードにより暗号化キーを解読する。受信機３６はリンク１００を介して受信された暗号化（インサイファ）された乱数から暗号化（スクランブル）された信号を分離しかつ暗号化された乱数を解読装置（デイサイファラ）３２から受信されたキーによ

り解読される解読装置３４に供給する。解読された乱数およびキーは次いで組み合わされかつ送信機におけると同様な方法でシーケンス発生器をリセットまたは「シード（seed）」するようにＰＮシーケンス発生器３８に付加され、それによりＳＳＴＶ送信機の信号処理装置２４において暗号化するのに使用されたと同一の分けられた（セグメントされた）ＰＮシーケンスを結果として生ずる。この分けられたＰＮシーケンスは次に受信されたプログラム信号を解読（デイスクランブル）するのに使用される信号処理装置４０に供給される。解読された信号は次に加入者のテレビセット４２に供給される。

【００１８】上述した防護装置は分けられた偽乱数（ＰＮ）シーケンスを発生しかつ同期させる新規の技術および安全なキー分配方法を提供する。発生された分割ＰＮシーケンスはプログラム信号を暗号化（スクランブル）しかつ解読（デイスクランブル）する映像および音声信号処理装置を制御するのに使用される。異なる分割ＰＮシーケンスが各々の異なるキーによって発生されるので、暗号化シーケンスは各々のキーについて異なり、そしてキーを周期的に変えることにより、暗号化および解読シーケンスは変えられる。したがって、如何なる者も解読装置によってかまたはそれによらず受信されたプログラム信号を現在のキーの正確な知識なくしては解読することができない。

【００１９】各々の一定の持続時間のため、特定のチャンネルは任意に選択された数およびその月のキーによって発生されるＰＮシーケンスによって解読（デイスクランブル）される。異なるチャンネルの加入者が彼らの間でキーを交換するのを防ぐために、各加入者に分配される一定のチャンネルが異なるようにすることが必須であり、そしてこれは各加入者の唯一のユーザーＩＤコードでキーを暗号化することにより達成される。この方法においては、単一のキーが如何なる時間においてもレジスタ１４によって供給されるけれども、異なるキーが各加入者によって要求される。加入者の特別なキーが受像機に挿入されるときのみレジスタ１４に含まれるその月の実際のキーが解読装置３４およびシーケンス発生器３８に供給されることができ、そして解読装置３２内でその月の実際のキーの解読が加入者の受像機の内部でかつ加入者の知見なしに行なわれる。

【００２０】防護装置の重要な特徴は正当な加入者が短かい時間周期内で同期を得ねばならないということである。本発明による装置において信号処理装置２４および４０で信号を暗号化しかつ解読するのに使用されるＰＮシーケンスはその各々がその月のキーと例えば毎秒で変化する乱数との組み合わせによってシードされる短かいセグメントに分離される。したがって、正当な加入者が彼の特有のキーを所持すると見做せば、同期を得るのに要する時間は同期が停電、暴風雨、チャンネルの変化等による同期損失の場合に迅速に得られることができるように各乱数の持続時間に実質上等しい。

【００２１】本発明による防護装置における個々の構成要素は従来公知であり、そしてそれらの構成要素の内部詳細は本発明の一部を構成しないのでここでは詳細に説明されない。その月のキーおよび乱数を暗号化するのに使用される暗号化装置（インサーファラ）は２つの異なる暗号化装置にすることができるが、受信側でのハードウエアの簡単化、および加入者受信機の大量生産において結果として生ずるコスト節減のため、同一の暗号化装置が使用されることが好ましい。この暗号化装置はそれが十分に高いレベルの安全性を有する限り如何なる暗号化方法にも使用することができる。

【００２２】ＰＮシーケンス発生器は、同様に十分な安全度を有する限り如何なる一般的なＰＮシーケンス発生器を用いることもでき、例えば適当に選択された非直線フイードバックシフトレジスタで間に合うかも知れない。送信機中の乱数発生器は「本当の」乱数を発生する公知の熱的雑音発生器であっても良く、またはデジタルエレクトロニクスまたはコンピュータのソフトウエアにより公知の方法で履行されるシーケンス発生器１８と同様な偽乱数発生器であっても良い。同様に、ＰＮシーケンス発生器１８および３８用の「シード」を発生するようにその月のキーと乱数発生器を組み合わせる技術は重要ではなく、最も簡単な技術によれば２つの数のビット・バイ・ビット・モジュール２の加算である。

【００２３】一般に、図中の各機能ブロックはそれらの特別な履行に依存する現存の技術により、装置の複雑さおよびコストおよび安全度によって達成されることができる。簡単な暗号化装置の変換は各チャンネルまたは特別なプログラムに関して異なる変数によって特定されそして月ごとに変化させられる。

【００２４】各加入者セット内のユーザーＩＤコード３０は１組の２進スイッチかまたは加入者が数を見るかまたは変えることを阻止するように密封ボックス内の読出し専用メモリにプログラムされたビットパターンであっても良い。非直線フイードバックシフトレジスタに加えて簡単な暗号化装置を使用することは装置の複雑さを不必要に増大すると思うかも知れない。しかしながら、少量のデータ、すなわち「シード」のみが各時間に処理される必要がありかつ暗号化装置の統計的特性がＰＮシーケンス発生器の出力を締め付けないので、この暗号化装置は非常に簡単にすることができる。

【００２５】例えば、１つの考え得るアプローチは、暗号フイードバックを有するかまたはそれを有していないランダムビットのＲＯＭＳテーブルである。この簡単な暗号化装置の使用は暗号同期およびキー分配の問題を非常に簡単化し、かつそれゆえ、装置全体の複雑さを減少する。プログラム信号の暗号化の適宜の選択は、オン－オフスイッチング、任意変換ライン、フイールドまたはフレーム、および幾つかの任意に固定のステップによる

遅延水平ラインまたはフィールドのごとき通常の暗号化技術を含んでいる。いずれの場合でも、使用される技術は送信および受信側双方で同期されねばならないＰＮシーケンスの発生を必要とする。

【図面の簡単な説明】

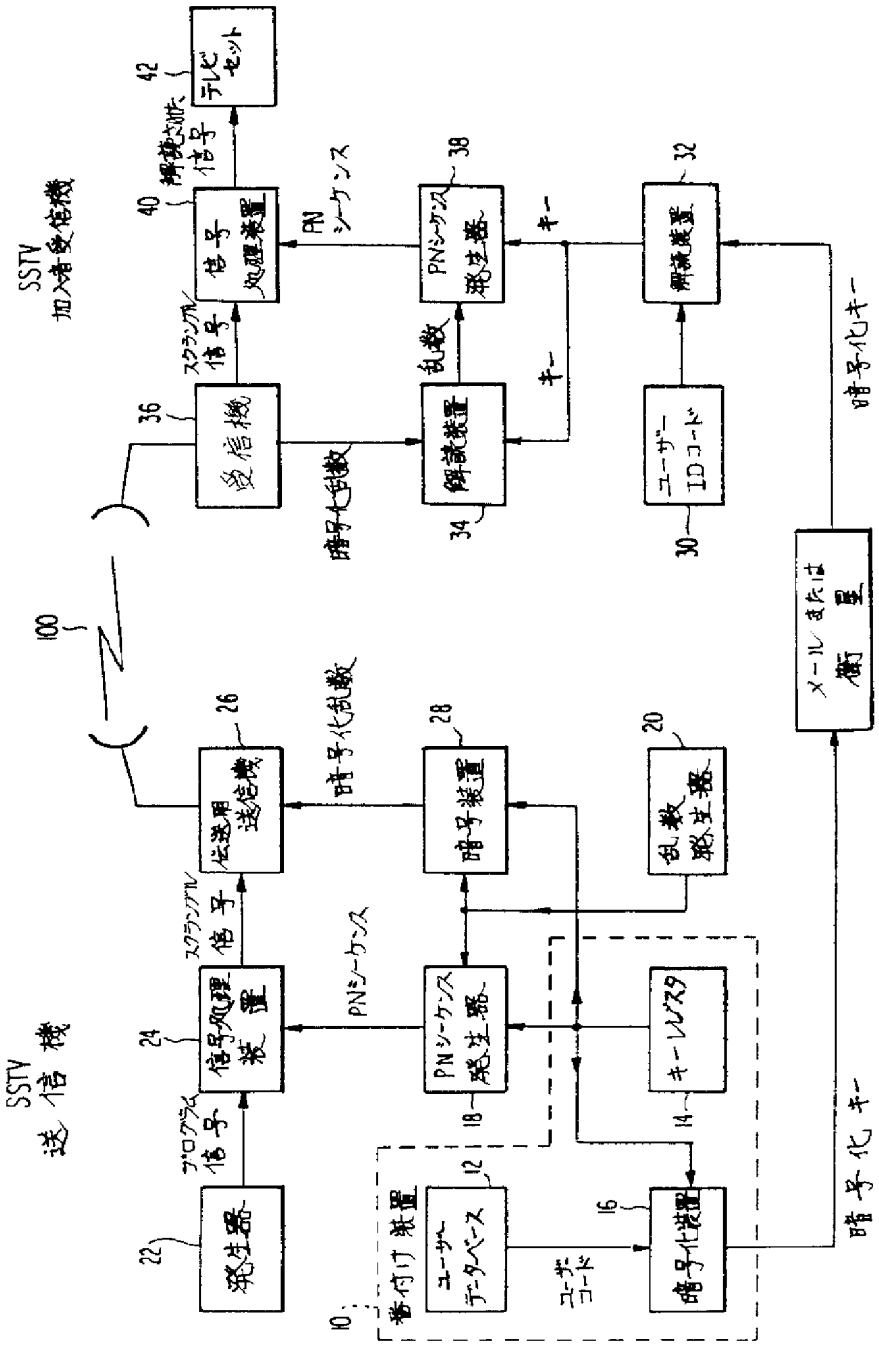
【図１】図１は、本発明によるＳＳＴＶ防護装置の必須構成要素を示すブロック図である。

【符号の説明】

１０　番付け装置
１２　ユーザーデータベース
１４　キーレジスタ
１６　暗号化装置

１８，３８　ＰＮシーケンス発生器
２０　乱数発生器
２２　発生器
２４　信号処理装置
２６　伝送用送信機
２８　暗号装置
３０　ユーザーＩＤコード
３２，３４　解読装置
３６　受信機
４０　信号処理装置
４２　テレビセット

【図１】



フロントページの続き

(72)発明者　ラツセル・ジエイ・フアン
アメリカ合衆国　メリーランド　20729、
ブルツクヴイル、トレツドウエイ・ロード
19321

United States Patent [19]

Lee et al.

[11] Patent Number: 4,484,027

[45] Date of Patent: Nov. 20, 1984

[54] **SECURITY SYSTEM FOR SSTV ENCRYPTION**

[75] Inventors: **Lin-nan Lee**, Germantown; **Russell J. Fang**, Brookeville, both of Md.

[73] Assignee: **Communications Satellite Corporation**, Washington, D.C.

[21] Appl. No.: **322,833**

[22] Filed: **Nov. 19, 1981**

[51] **Int. Cl.**[3] **H04L 9/02**; H04K 1/02

[52] **U.S. Cl.** **178/22.13**; 178/22.15; 178/22.16; 358/114; 358/122

[58] **Field of Search** 178/22.08, 22.13, 22.15, 178/22.09, 22.16; 358/114, 122; 340/706

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,649,915	3/1972	Mildonian, Jr.	455/26
3,659,046	4/1972	Angeleri et al.	178/22.13
3,801,732	4/1974	Reeves	358/124
3,911,216	10/1975	Barket et al.	178/22.15
3,914,534	10/1975	Forbes	358/122
4,058,830	11/1977	Guinet et al.	358/114
4,081,832	3/1978	Sherman	358/122
4,115,807	9/1978	Pires	358/122
4,163,254	7/1979	Block et al.	358/122
4,200,770	4/1980	Hellman et al.	178/22.11
4,292,650	9/1981	Hendrickson	358/122
4,310,720	1/1982	Check, Jr.	178/22.08
4,323,921	4/1982	Guillou	178/22.09
4,337,483	6/1982	Guillou	340/706
4,354,201	10/1982	Sechet et al.	358/122
4,365,110	12/1982	Lee et al.	178/22.09
4,388,643	6/1983	Aminetzah	178/22.08

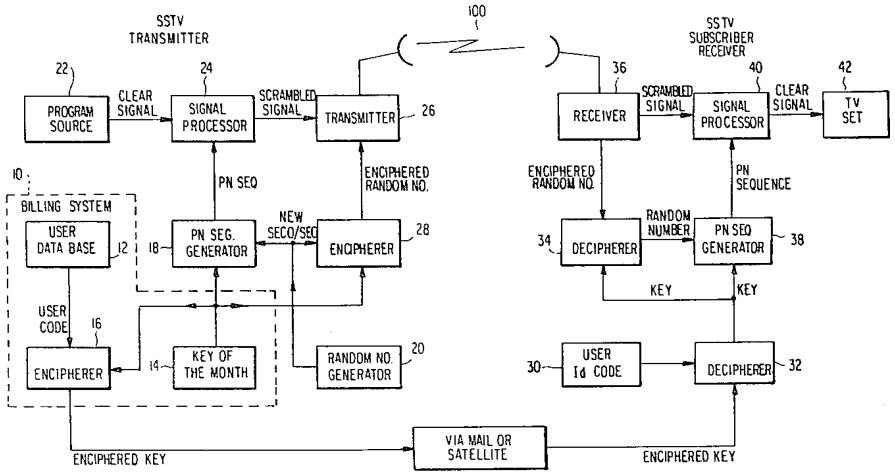
Primary Examiner—Sal Cangialosi

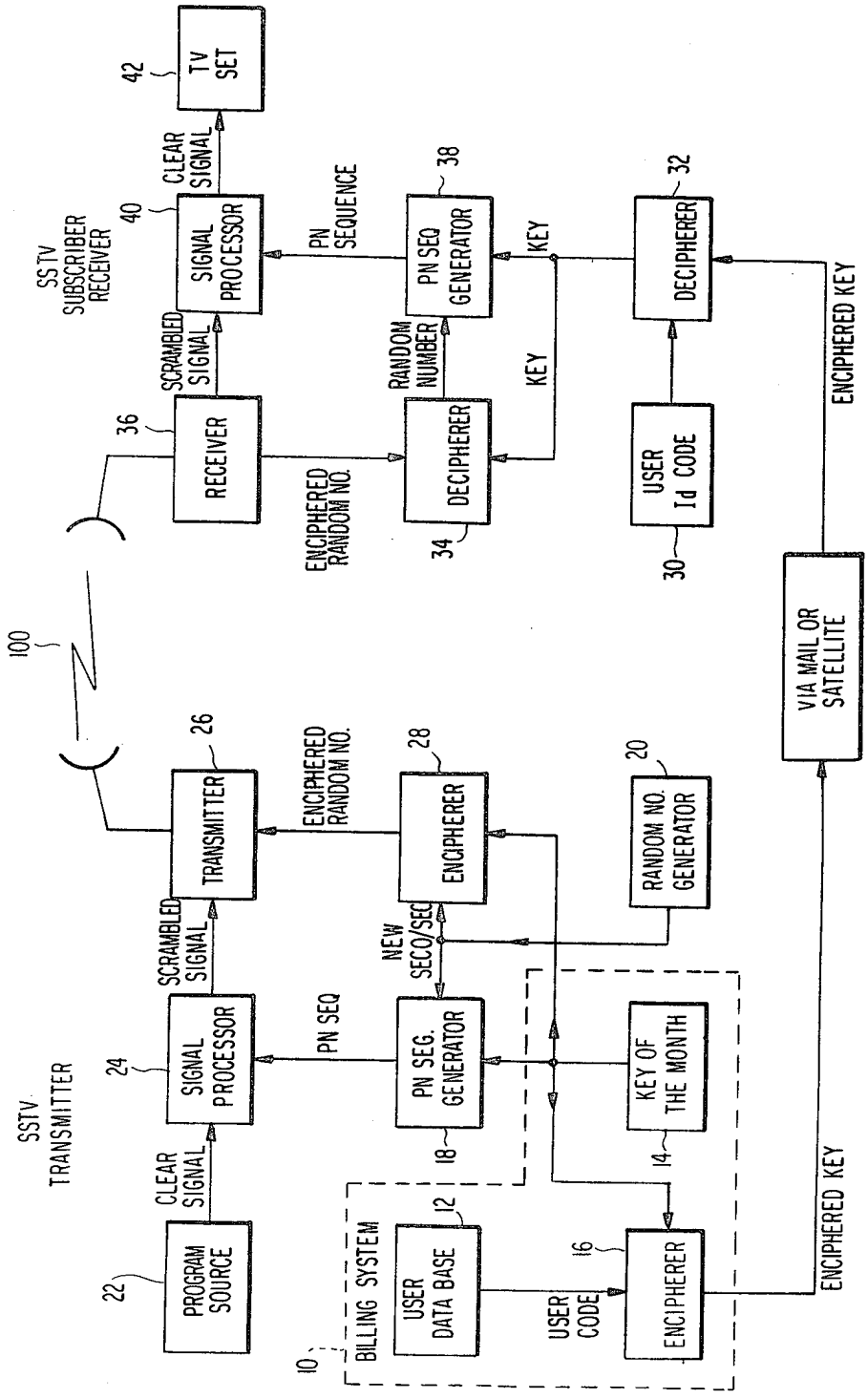
Attorney, Agent, or Firm—Sughrue, Mion, Zinn, Macpeak & Seas

[57] **ABSTRACT**

In a secure communications system, a key number which is changed periodically, e.g. monthly, and a random number from a random number generator are combined and used as a seed to reset a PN sequence generator, with the output of the generator being used to control encryption of transmission data in a signal processor. The key is also provided to a first encipherer to encipher the random number for transmission with the encrypted data. At the receiver, the key is provided on common to a decipherer for deciphering the random number and a PN sequence generator which is periodically reset by the combination of the key and random number in the same manner as in the transmitter. The PN sequence is then used to decrypt the information. User identification codes are stored in the transmitter and are used to encipher the key, with each employing its ID code to decipher the key. The user ID codes are known only to the system operator, so that not even a particular user can know the key.

19 Claims, 1 Drawing Figure




SSTV TRANSMITTER
SSTV SUBSCRIBER RECEIVER
100
PROGRAM SOURCE
22
CLEAR SIGNAL
SIGNAL PROCESSOR
24
SCRAMBLED SIGNAL
TRANSMITTER
26
ENCIPHERED RANDOM NO.
RECEIVER
36
SCRAMBLED SIGNAL
SIGNAL PROCESSOR
40
CLEAR SIGNAL
TV SET
42
BILLING SYSTEM
10
USER DATA BASE
12
USER CODE
PN SEQ
PN SEG. GENERATOR
18
NEW SECO/SEC
ENCIPHERER
28
ENCIPHERED RANDOM NO.
DECIPHERER
34
RANDOM NUMBER
PN SEQUENCE
PN SEQ GENERATOR
38
KEY
KEY OF THE MONTH
14
ENCIPHERER
16
RANDOM NO. GENERATOR
20
KEY
DECIPHERER
32
USER Id CODE
30
ENCIPHERED KEY
VIA MAIL OR SATELLITE
ENCIPHERED KEY

SECURITY SYSTEM FOR SSTV ENCRYPTION

BACKGROUND OF THE INVENTION

The present invention is related to the confidentiality of television signal transmissions, and more particularly to the protection of TV signal transmissions from unauthorized reception. The environment in which the present invention may be widely applicable, and in the context of which the invention will be described herein, is that of subscriber television and TV program distribution.

Subscriber television systems are becoming increasingly widespread wherein TV signals are sent out via a cable network or over the air and are intended for reception and viewing by only those subscribers who have paid a monthly fee. With the increase in subscriber television systems has also come an increase in the number of people attempting to receive and display the premium television programs without payment. Thus, there is a need for more sophisticated security techniques for preventing such unauthorized reception.

Many existing subscriber television systems utilize, directly or indirectly, signals transmitted via satellite, and it is becoming quite common for non-paying individuals to receive and display the premium television programs via television receive only (TVRO) antennas, thus resulting in a substantial loss of revenue for the distributors of the subscription television programs. In addition, various direct satellite broadcast television systems are currently being proposed wherein subscription television programs will be broadcast directly via satellite to individual subscriber homes. These subscription satellite television (SSTV) systems will be quite vulnerable to unauthorized reception, and an effective security technique is therefore highly desirable.

The purpose of a security subsystem for an SSTV system is to protect the distributor's business interest and, accordingly, the following objectives should be achieved:

(1) To prevent a non-subscriber from receiving intelligible video and audio signals by using a regular home television set;

(2) To prevent a delinquent subscriber from receiving intelligible video and audio signals by using the SSTV decoder;

(3) To prevent a legitimate subscriber from receiving intelligible video and audio signals of unsubscribed SSTV channels or programs;

(4) To discourage an average technician from building his own receiver capable of obtaining acceptable quality video and audio signals;

(5) To discourage a small unauthorized business concern from manufacturing and marketing devices which are capable of receiving and displaying acceptable quality video and audio signals from the SSTV channels; and

(6) To allow a legitimate subscriber to receive and display high quality video and audio signals from the subscribed channels or programs.

It would also be highly desirable to achieve the above objectives at a reasonable cost.

A number of security systems for CATV exist, most of which involve the suppression or removal of the horizontal sync pulses from the video signal before transmission, and the recovery of the sync pulses at the receive end. These techniques will prevent people without the sync recovery circuits from receiving and displaying the programs and may therefore achieve objectives (1) and (6) above, but those security systems do not achieve objectives (2) and (3) and, since sync recovery circuits are relatively easily designed and manufactured, also do not satisfy objectives (4) and (5).

More sophisticated techniques may include additional intelligence in the subscriber's decoder box, including the capability of receiving commands from a control center which are specifically addressed to an individual subscriber and are used to turn on or off some or all of the channels. These more sophisticated security techniques may succeed in achieving objectives (1)–(3) and (6), but still do not satisfy objectives (4) and (5). For example, most of these techniques involve the checking of a password, and a particular channel is turned on only if the password is matched. This could be relatively easily by-passed by modifying the subscriber's decoder box or building a separate box with all of the necessary features except the on/off switch. Further, subscribers may also be able to tamper with the decoder box to receive more programs than are actually paid for.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a security subsystem for a subscription television system wherein all of the above-mentioned objectives (1)–(6) are achieved.

It is a further object of this invention to provide such a security subsystem of minimal cost and complexity.

These and other objects are achieved according to the present invention by using a cryptographic technique for scrambling and descrambling of the video signals. The scrambling and descrambling techniques utilize a "key" which is changed on a regular basis and is sent only to paid subscribers, and even this "key" is sent in a different encrypted form to each subscriber so that delinquent subscribers cannot learn the current key from others.

A record is kept of unique user ID codes corresponding to each subscriber, and in a transmitter according to the preferred embodiment of this invention, the key is ciphered with each subscriber's unique ID code prior to sending the key to that subscriber. A random number generator in the transmitter generates a new random number at regular intervals, for example, every second, and this number is combined with the key, and the combined number is then used as a seed to reset a PN sequence generator every second. This PN sequence generator will thus generate a PN sequence with a random seed in one-second segments, and the segmented PN sequence is supplied to a signal processor where it is used to scramble the audio and video program signals. The random number generator is also ciphered with the key and the enciphered random number is continually transmitted with the scrambled video signal.

At the receiver, the enciphered key, which has been sent either via satellite or mail, is deciphered in the receiver utilizing the particular subscriber's unique ID code, which ID code is internal to the receiver and is unknown to the subscriber. The deciphered key is then in turn used to decipher the enciphered random number received with the scrambled program signal. The deciphered key and random number are then combined as in the transmitter, and the combined signal is used to continually reset a PN sequence generator identical to that in the transmitter so that a segmented PN sequence will

be generated in the receiver which is identical to that generated in the transmitter, and this segmented PN sequence can then be used to descramble the received signal. The descrambled signal will then be supplied to the subscriber television set.

BRIEF DESCRIPTION OF THE DRAWING

The invention will be more clearly understood with reference to the following description in conjunction with the accompanying drawing wherein the single FIGURE is a block diagram of the essential components of the SSTV security system according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The drawing illustrates a functional block diagram of the SSTV security system according to this invention. The SSTV transmitter will typically include or have access to a billing system computer **10** which will store subscriber information including a list of paid subscribers and their corresponding unique user ID codes. This information may typically be stored in a user data base **12** within the computer. Also within the computer will be a register **14** or the like containing a key which will be changed on a regular basis, e.g. monthly. In preparation for sending this "key of the month" to each current subscriber, the key is enciphered in an encipherer **16** with the user ID code unique to that particular current subscriber, and the enciphered key is then sent to the subscriber.

The transmitter includes a pseudo-random number (PN) sequence generator **18** and a random number generator **20**. The random number generator **20** periodically generates a new random number, e.g. once every second, and the outputs of the random number generator **20** and key register **14** are combined and loaded into the PN sequence generator **18** to periodically reset or "seed" the PN sequence generator **18** in a manner well known in the art. Each seeding of the sequence generator **18** will begin a new segment of the PN sequence. The program signal from source **22** is supplied to a signal processor **24** where it is encrypted with the segmented PN sequence from generator **18**. The encryption technique used may be any one of a variety of well known techniques and need not be discussed in detail herein. The encrypted, or scrambled, signal is then provided to a transmitter **26** for transmission over link **100** to the various subscriber receivers.

The random number from generator **20** is enciphered with the key of the month in an encipherer **28**, and the enciphered random number is transmitted with the scrambled video signal over the link **100**.

At the receiver, a register **30** or the like internal to the subscriber TV receiver contains a subscriber-specific secret user ID code which is set prior to installation and is stored in the user data base **12** of the billing computer at the transmitter. Thus, when the subscriber receiver receives the enciphered key or when the user receives the enciphered key by mail and enters the enciphered key into the receiver, a decipherer **32** in the receiver deciphers the enciphered key with the secret user ID code specific to that particular subscriber, and the deciphered key is provided to a decipherer **34**. A receiver **36** separates the scrambled signal from the enciphered random number received over link **100** and provides the enciphered random number to the decipherer **34** where it is deciphered with the key received from the decipherer **32**. The deciphered random number and key are then combined and loaded into the PN sequence generator **38** to reset or "seed" the sequence generator in the same manner as in the transmitter, to thereby result in the same segmented PN sequence as was used for scrambling in the SSTV transmitter signal processor **24**. This segmented PN sequence is then provided to signal processor **40** where it is used to descramble the received program signal. The descrambled signal is then provided to the subscriber television set **42**.

The above-described security system provides a novel technique for generating and synchronizing a segmented pseudo-random number (PN) sequence, and a secure key distribution method. The segmented PN sequence generated is used to control the video and audio signal processors that scramble and descramble the program signals. Since a different segmented PN sequence will be generated by each distinct key, the scrambling sequence is different for each key, and by periodically changing the key the scrambling and descrambling sequences will change. Thus, it is not possible for anyone without exact knowledge of the current key to descramble the received program signal with or without a descrambling device.

For each given duration of time, a particular channel is scrambled by a PN sequence that is generated by a randomly selected number and the key of the month. To prevent subscribers of different channels from exchanging the keys among themselves, it is essential that the key for a given channel distributed to each subscriber look different, and this accomplished by enciphering the key with each subscriber's unique user ID code. In this way, although a single key is provided by the register **14** at any one time, a different key is required by each subscriber. It is only when the subscriber-specific key is entered into the receiver that the true key of the month contained in register **14** can be provided to the decipherer **34** and sequence generator **38**, and the deciphering of this true key of the month in the decipherer **32** is performed internally of the subscriber receiver and without the subscriber's knowledge.

An important feature of any security system is that a legitimate subscriber must be capable of obtaining synchronization within a short period of time. In the system according to the present invention, the PN sequence used for scrambling and descrambling the signal in signal processors **24** and **40**, respectively, is separated into short segments each of which is seeded by the combination of the key of the month and a random number which changes, for example, once every second. Thus, assuming that a legitimate subscriber does have his appropriate key, the time required to acquire synchronization will be substantially equal to the duration of each random number so that synchronization can be acquired rapidly in case of loss of sync due to power outages, rainstorms, changing of channels, etc.

The individual components in the security system according to the present invention are known in the art and need not be described in detail herein since the internal details of these components do not constitute a part of the present invention. The encipherers used to encipher the key of the month and the random number can be two different encipherers, but for the sake of hardware simplicity at the receive side, and consequent cost savings in mass production of the subscriber receivers, it is preferable that the same encipherers be used. The encipherer may employ any enciphering method as long as it has a sufficiently high level of security.

The PN sequence generator can be any general PN sequence generator as long as it also has sufficient security strength, e.g. a properly selected non-linear feedback shift register may suffice.

The random number generator in the transmitter may be a well known thermal noise generator which generates "true" random numbers, or it may be a pseudo-random number generator similar to the sequence generator **18**, implemented in a well known manner with digital electronics or computer software. Similarly, the technique for combining the key of the month and the random number generator to produce the "seed" for the PN sequence generators **18** and **38** is not critical, with the simplest technique being a bit-by-bit modulo-2 addition of the two numbers.

In general, each of the functional blocks in the drawing can be implemented with existing techniques, with system complexity and cost and security strength depending on the particular implementation of each of the functional blocks.

The transformation of the simple cipherer is specified by a variable which is different for each channel or special program, and is changed every month.

The user ID code **30** within each subscriber set may be a set of binary switches or a bit pattern programmed into a read-only memory in a sealed box to prevent the subscriber from seeing or changing the number.

The use of a simple cipherer in addition to the non-linear feedback shift-register may seem to increase the system complexity unnecesarily. However, since only a small amount of data, namely the "seed", need be handled each time, and since the statistical properties of the cipherer do not impact to the output of the PN sequence generator, the cipherer can be very simple. One possible approach, for example, is a ROM table of random bits with or without cipher feedback. The use of this simple cipherer greatly simplifies the problem of cryptosynchronization and key distribution, and therefore reduces the overall system complexity.

Suitable alternatives for the scrambling of the program signals include conventional scrambling techniques such as on-off switching, randomly inverting lines, fields or frames, and delaying horizontal lines or fields by certain randomly fixed steps. In any case, the technique used will require the generation of a PN sequence which must be synchronized at both the transmit and receive sides.

What is claimed is:

1. In a communications system including a transmitter and a receiver, said transmitter including a program source for providing a program signal representing program information, a transmit signal processor for encrypting said program signal in accordance with a transmit control signal and transmit means for transmitting said encrypted signal, said receiver including receive means for receiving said encrypted signal, a receiver signal processor for decrypting said encrypted signal in accordance with a receive control signal and means for receiving said decrypted signal and providing said program information, the improvement comprising:

first generator means at said transmitter for generating a first sequence of signals representing a first sequence of numbers;

key number means at said transmitter for providing a key number signal representing a key number;

second generator means at said transmitter for generating a second sequence of signals representing a second sequence of numbers, said second generator means being periodically reset by a reset signal comprising the output of said first generator means to thereby generate a plurality of sequence segments each beginning with a reset signal, the output of said second generator means comprising said transmit control signal;

means at said transmitter for enciphering said first sequence of signals with said key number signal and for providing said enciphered first signal sequence to said transmit means for transmission with said encrypted program signal;

means at said receiver for providing said key number signal;

receive deciphering means at said receiver for receiving said enciphered first signal sequence and said key number, deciphering said first signal sequence in accordance with said key number and providing said deciphered first signal sequence as an output; and

receive generating means for generating a sequence of signals representing said first sequence of numbers, said receive generating means being periodically reset by a reset signal comprising the output of said receive deciphering means to thereby generate said plurality of sequence segments, said plurality of sequence segments being provided by said receive generating means to said receive signal processor as said receive control signal.

2. A communications system as defined in claim **1**, further comprising:

means for providing an identification number signal uniquely identifying said receiver;

means for enciphering said key number signal with said identification signal;

means at said receiver for providing said identification number signal; and

means at said receiver for receiving said identification number signal and said enciphered key number signal and for deciphering said key number signal, said deciphered key number signal being provided to said receive deciphering means.

3. A communications system as defined in either one of claims **1** or **2**, wherein each of said reset signals provided to said second generator means comprises a combination of said key number signal and a signal of said first signal sequence, and wherein each of said reset signals provided to said receive generator means comprises a combination of said key number signal and a signal of said deciphered first signal sequence.

4. A communications systems as defined in claim **3**, wherein said key number signal is changed at predetermined time intervals.

5. A communications system as defined in claim **4**, wherein said second generator means is a non-linear pseudorandom sequence generator.

6. A communications system as defined in claim **3**, wherein a plurality of receivers receive the encrypted signal transmitted by said transmitter, each of said receivers having a corresponding unique identification number and said enciphered key number received at each receiver being enciphered with the user identification number unique to said each receiver.

7. The communications system as defined in claim **6**, wherein said first signal sequence represents a substantially random number sequence.

8. In a method of providing security in a signal transmission system, said method including the steps of en-

crypting in accordance with an encryption control signal a program signal representing information, transmitting said encrypted signal, receiving said encrypted signal, decrypting said received encrypted signal in accordance with a decryption control signal and providing said information represented by said decrypted signal, the improvement comprising:

generating a key number signal representing a key number;

generating a first signal sequence representing a first sequence of numbers;

generating a second signal sequence representing a second sequence of numbers, said second signal sequence being periodically reset by a reset signal comprising a signal of said first signal sequence to thereby generate a plurality of second sequence segments;

providing said second sequence segments to said transmit signal processor as said encryption control signal;

enciphering said first signal sequence with said key number and providing said enciphered first sequence to said transmitter for transmission with said encrypted signal;

decrypting said enciphered first sequence at said receiver in accordance with said key number signal;

generating said second sequence segments at said receiver by resetting a receive number signal generator with a reset signal comprising said deciphered first signal sequence; and

providing said second sequence segments to said receive signal processor as said decryption control signal.

9. A method as defined in claim **8**, further comprising:

enciphering said key number signal at said transmitter with a user identification number signal uniquely identifying said receiver;

transmitting said enciphered key number signal to said receiver;

deciphering said enciphered key number signal at said receiver in accordance with said user identification number signal uniquely identifying said receiver; and

providing said deciphered key number signal to said deciphering means.

10. The method as defined in claim **9**, further comprising the steps of:

combining said key number signal and a signal in said first sequence to obtain said reset signal in said transmitter; and

combining said key number signal and a signal in said deciphered first sequence in order to obtain said reset signal in said receiver.

11. The method as defined in any one of claims **8–10**, further comprising the step of periodically changing said key number signal.

12. The method as defined in claim **11**, wherein said second generator means in said transmitter and said generator means in said receiver each generate non-linear pseudo-random signal sequences.

13. The method as defined in claim **12**, wherein said first signal sequence represents a substantially random number sequence.

14. A communications system including a transmitter and a receiver, said system comprising:

a program source at said transmitter for providing a program signal representing program information;

first generator means at said transmitter for generating a first sequence of signals representing a first sequence of numbers;

key number means at said transmitter for providing a key number signal representing a key number;

transmit signal processing means at said transmitter responsive to at least said first sequence of signals for encrypting said program signal;

enciphering means at said transmitter for enciphering said first sequence of signals with said key number signal to provide an enciphered first signal sequence;

transmit means at said transmitter for transmitting said encrypted program signal and said enciphered first signal sequence;

means at said receiver for providing said key number signal;

receive deciphering means at said receiver for receiving said enciphered first signal sequence and said key number, deciphering said first signal sequence in accordance with said key number and providing said deciphered first signal sequence as an output; and

receive generating means at said receiver responsive to at least said output of said receive deciphering means for receiving and decrypting said encrypted program signal to obtain said program signal.

15. A communications system as defined in claim **14**, wherein said transmit signal processing means includes encryption means for encrypting said program signal in accordance with an encryption control signal, and second generator means at said transmitter for generating a second sequence of signals representing a second sequence of numbers, said second generator means being periodically reset by a reset signal comprising at least the output of said first generator means to thereby generate a plurality of sequence segments each beginning with a reset signal, the output of said second generator means comprising said encryption control signal.

16. A communications system as defined in claim **15**, wherein said reset signal comprises a combination of said key number signal and the output of said first generator means.

17. A method of providing security in a signal transmission system between a transmitter and a receiver, said method comprising the steps of:

providing a program signal representing information;

generating a first sequence of signals representing a first sequence of numbers;

providing a key number signal representing a key number;

encrypting said program signal in accordance with at least said first sequence of signals;

enciphering said first sequence of signals with said key number signal to provide an enciphered first signal sequence;

transmitting said encrypted program signal and said enciphered first signal sequence to said receiver;

providing said key number signal at said receiver;

deciphering said first signal sequence at said receiver in accordance with said key number to obtain a deciphered first signal sequence; and

decrypting said encrypted program signal at said receiver in accordance with at least deciphered first signal sequence to obtain said program signal.

18. A method as defined in claim **17**, wherein said step of encrypting said program signal in accordance with at least said first sequence of signals comprises the steps

generating a second sequence of signals representing a second sequence of numbers, said second sequence of signals comprising a plurality of sequence segments each beginning with a reset signal, said reset signal comprising at least said first signal sequence, said encrypting said program signal in accordance with said second sequence of signals.

19. A method as defined in claim **18**, wherein said reset signal comprises a combination of said key number signal and said first sequence of signals.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 4,484,027

DATED : November 20, 1984

INVENTOR(S) : Lin-nan LEE, et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 2, line 2, "those" should be --these--.

Column 9, line 5, "said" (second occurrence) should be --and--.

Signed and Sealed this

Tenth Day of *September 1985*

[SEAL]

Attest:

DONALD J. QUIGG

Attesting Officer *Acting Commissioner of Patents and Trademarks - Designate*